(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－171887

(43)公開日　平成10年(1998)６月26日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３３０
			３４０Ｚ

審査請求　未請求　請求項の数13　ＯＬ　（全 17 頁）

(21)出願番号　特願平8－333387

(22)出願日　平成８年(1996)12月13日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　広谷　政彰
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　千葉　寛之
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所ビジネスシステム開発センタ内

(74)代理人　弁理士　小川　勝男

最終頁に続く

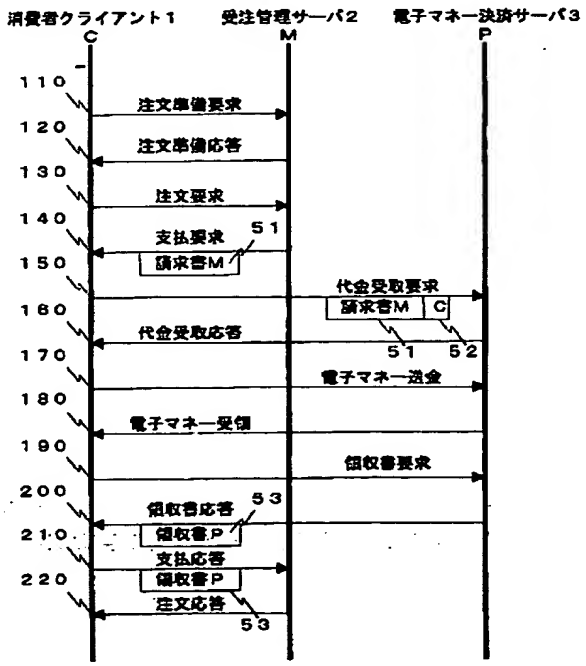
(54)【発明の名称】　オンラインショッピングシステム

(57)【要約】

【課題】　電子マネーを利用して取引する場合に，取引内容や決済が完了したことを客観的に証明できる電子データをオープンネットワーク上で提供する．

【解決手段】　購入プロセスでは，受注管理サーバに請求書データを発行する手段と，電子マネー決済サーバに領収書データを発行する手段を設け，消費者クライアントは発注し，受注管理サーバから請求書データを受信し，データを電子マネー決済サーバに送信後，電子マネーを送信し電子マネー決済サーバから受信して領収書データを受注管理サーバに送信して取引が完了する．払戻プロセスでは，受注管理サーバに払戻許可書データを発行する手段と，消費者クライアントに払戻領収書を発行する手段を設け，消費者クライアントが払戻許可書を受信すると，データを電子マネー決済サーバに送信し，電子マネー決済サーバから電子マネーを受領し，電子マネー決済サーバに払戻領収書データを送信し払戻が完了する．

図5



1

【特許請求の範囲】

【請求項１】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて，第１の情報処理装置は，注文データなどを入力するための手段と，注文データと請求書データと領収書データを表示するための手段と，注文データを送信するための手段と，請求書データと領収書データを送受信するための手段と，電子マネーを格納するための手段と，電子マネーを送受信するための手段を有し，第２の情報処理装置は前記注文データを受信するための手段と，前記注文データを記憶するための手段と，少なくとも支払先である第３の情報処理装置を特定するためのデータと取引を特定するための識別子と支払金額で構成されるデータに前記第２の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した請求書データを発行するための手段と，前記請求書データを送信するための手段と，領収書データを受信する手段と，前記領収書データに添付されているデジタル署名が前記請求書データで指定した支払先が有する秘密鍵でデジタル署名されたものかどうかをチェックするための手段を有し，第３の情報処理装置は，電子マネーを格納する手段と，電子マネーを送受信するための手段と，決済データを記憶するための手段と，少なくとも領収金額と取引を特定するための識別子で構成されるデータに第３の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した領収書データを発行する手段と，前記領収書データを送信するための手段を有することを特徴とするオンラインショッピングシステム。

【請求項２】請求項１記載のオンラインショッピングシステムにおいて，前記第１の情報処理装置が前記第２の情報処理装置に注文データを送信するステップと，前記第２の情報処理装置が前記注文データを受信した場合に前記請求書データを発行して前記第１の情報処理装置に送信するステップと，前記第１の情報処理装置が前記請求書データを受信すると前記第３の情報処理装置に前記請求書データを送信するステップと，前記第３の情報処理装置の応答に対して前記第１の情報処理装置から前記第３の情報処理装置に電子マネーを送金するステップと，前記第３の情報処理装置が前記電子マネーを受信したら前記領収書データを発行して前記第１の情報処理装置に送信するステップと，前記第１の情報処理装置が前記領収書データを受信したら，前記領収書データを前記第２の情報処理装置に送信するステップを有することを特徴とするオンラインショッピングシステム。

【請求項３】請求項２記載のオンラインショッピングシステムにおいて，前記第１の情報処理装置が前記第３の情報処理装置に請求書データを送信するステップの前に，前記請求書データを含む前記ステップで送信するデータに前記第１の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付するステップを追加することを

2

特徴とするオンラインショッピングシステム。

【請求項４】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて，第１の情報処理装置は注文データなどを入力するための手段と，注文データと請求書データと領収書データを表示するための手段と，電子マネーを格納するための手段と，電子マネーを送受信するための手段と，注文データを送信するための手段と，請求書データと領収書データを送受信する手段を有し，かつ前記第１の情報処理装置は，第２の情報処理装置に注文データを送信するステップと，前記第２の情報処理装置から請求書データを受信すると第３の情報処理装置に前記請求書データを送信するステップと，前記第３の情報処理装置からの応答に応じて前記第３の情報処理装置へ電子マネーを送信するステップと，前記第３の情報処理装置から領収書データを受信すると前記領収書データを前記第２の情報処理装置に送信するステップを有することを特徴とするオンラインショッピングシステム。

【請求項５】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて，第２の情報処理装置は，注文データを受信する手段と，前記注文データを記憶するための手段と，少なくとも支払先を特定するためのデータと取引を特定するための識別子と支払金額で構成されるデータに前記第２の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した請求書データを発行する手段と，前記請求書データを送信するための手段と，領収書データを受信するための手段と，前記領収書データに添付されているデジタル署名が前記請求書データで指定した支払先が有する秘密鍵によってデジタル署名されたものかどうかをチェックするための手段を有し，第２の情報処理装置は，第１の情報処理装置から注文データを受信した場合に前記請求書データを発行するステップと前記請求書データを前記第１の情報処理装置に送信するステップを有し，さらに領収書データを受信した場合に前記領収書データが前記請求書データで指定した支払先によってデジタル署名されたものであることを判断するステップを有することを特徴とするオンラインショッピングシステム。

【請求項６】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて，第３の情報処理装置は，請求書データを受信するための手段と，決済データを記憶するための手段と，少なくとも領収金額と取引を特定するための識別子で構成されるデータに前記第３の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した領収書データを発行する手段と，電子マネーを格納するための手段と，電子マネーを送受信するための手段を有し，前記第３の情報処理装置は，第２の情報処理装置が発行した請求書データを第１の情報処理装置から受信するステップと，前記請求書データの有効性をチェックするステップと，前記請求書

データが有効である場合に前記第１の情報処理装置に送金許可を送信するステップと，前記第１の情報処理装置から電子マネーを受信したら領収書データを発行するステップと，前記領収書データを前記第１の情報処理装置に送信するステップを有することを特徴とするオンラインショッピングシステム。

【請求項７】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて，第１の情報処理装置は，少なくとも取引を特定するためのデータを含む払戻要求を送信する手段と，電子マネーを格納するための手段と，電子マネーを送受信するための手段と，少なくとも取引を特定するための識別子と受領した払戻金額に関するデータで構成されるデータにデジタル署名を添付した払戻領収書を発行するための手段と，前記払戻領収書を送信するための手段と，払戻許可データを送受信するための手段を有し，第２の情報処理装置は，前記払戻要求を受信するための手段と，注文データを記憶するための手段と，少なくとも払戻を行う第３の情報処理装置を特定するためのデータと払戻金額に関するデータと払戻を受領する人もしくは払戻を受領する第１の情報処理装置を特定するためのデータで構成されるデータにデジタル署名を添付した払戻許可データを発行するための手段と，前記払戻データを送信するための手段を有し，第３の情報処理装置は，前記払戻許可データを受信するための手段と，前記払戻許可データの有効性をチェックするための手段と，電子マネーを格納するための手段と，電子マネーを送受信するための手段と，決済データを記憶するための手段を有することを特徴とするオンラインショッピングシステム。

【請求項８】請求項７記載の払戻領収書の払戻を受領する人もしくは払戻を受領する第１の情報処理装置を特定するためのデータが，デジタル署名の正当性を証明するために使用される認証局に登録されている証書データに含まれる人もしくは情報処理装置を特定するためのデータであることを特徴とするオンラインショッピングシステム。

【請求項９】請求項７記載のオンラインショッピングシステムにおいて，前記第１の情報処理装置が前記第２の情報処理装置に払戻要求を送信するステップと，前記第２の情報処理装置が前記払戻要求を受信した場合に前記払戻許可データを発行して前記第１の情報処理装置に送信するステップと，前記第１の情報処理装置が前記払戻許可データを受信すると前記第３の情報処理装置に前記払戻許可データを送信するステップと，前記払戻許可データが有効である場合に前記第３の情報処理装置から前記第１の情報処理装置に電子マネーを送金するステップと，前記第１の情報処理装置が前記電子マネーを受信したら前記第３の情報処理装置に払戻領収書データを送信するステップ有することを特徴とするオンラインショッピングシステム。

【請求項１０】請求項９記載のオンラインショッピングシステムにおいて，前記第１の情報処理装置が前記第３の情報処理装置に前記払戻許可データを送信するステップの前に，前記払戻許可データを含む前記ステップで送信するデータに前記第１の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付するステップを追加することを特徴とするオンラインショッピングシステム。

【請求項１１】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて，第１の情報処理装置は，少なくとも取引を特定するためのデータを含む払戻要求を送信する手段と，電子マネーを格納するための手段と，電子マネーを送受信する手段と，少なくとも取引を特定するための識別子と受領した払戻金額に関するデータで構成されるデータにデジタル署名を添付した払戻領収書を発行するための手段と，前記払戻領収書を送信するための手段と，払戻許可データを送受信するための手段を有し，前記第１の情報処理装置は，払戻要求を送信するステップと，第２の情報処理装置から前記払戻許可データを受信した場合に，前記払戻許可データに前記第１の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付して第３の情報処理装置に送信するステップと，前記第３の情報処理装置から電子マネーを受信するステップと，前記電子マネーを受信した場合に払戻領収書データを発行するステップと，前記払戻領収書を前記第３の情報処理装置に送信するステップを有することを特徴とするオンラインショッピングシステム。

【請求項１２】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて，第２の情報処理装置は，前記払戻要求を受信するための手段と，注文データを記憶するための手段と，少なくとも払戻を行う第３の情報処理装置を特定するためのデータと払戻金額に関するデータと払戻を受領する人もしくは払戻を受領する第１の情報処理装置を特定するためのデータで構成されるデータにデジタル署名を添付した払戻許可データを発行する手段と，前記払戻データを送信するための手段を有し，第２の情報処理装置は，第１の情報処理装置から払戻要求を受信した場合に前記払戻許可データを発行するステップと前記払戻許可データを前記第１の情報処理装置に送信するステップと，前記第３の情報処理装置に払戻完了状態を問い合わせるステップを有することを特徴とするオンラインショッピングシステム。

【請求項１３】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて，第３の情報処理装置は，前記払戻許可データを受信するための手段と，前記払戻許可データの有効性をチェックするための手段と，電子マネーを格納するための手段と，電子マネーを送受信するための手段と，決済データを記憶するための手段を有し，前記第３の情報処理装置は，

第２の情報処理装置が発行した払戻許可データを第１の情報処理装置から受信するステップと，前記払戻許可データの有効性をチェックするステップと，前記払戻許可データが有効である場合に前記第１の情報処理装置に電子マネーを送信するステップと，前記第１の情報処理装置から払戻領収書データを受信するステップと，前記第２の情報処理装置から払戻完了状態の問合せがあった場合に，前記第２の情報処理装置に払戻完了状態を送信するステップを有することを特徴とするオンラインショッピングシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】インタネットなどのオープンなネットワークで電子マネーを利用して安全に取引するためのシステムに関する

【０００２】

【従来の技術】現在，インタネットなどのオープンなネットワークを使用してショッピングを行なうシステムが台頭してきている．既存のシステムでは，小売店はＷＷＷ(World Wide Web)サーバで商品情報を消費者に提供し，消費者はＷＷＷブラウザーで商品情報を見て購入したい商品を選択し，注文を出している．決済手段としては，クレジットカードを使用する方法と電子マネーを使用する方法が主流である．インタネットショッピングで問題になるのはセキュリティである．インタネットは誰でも簡単にアクセスできるために，第三者によって盗聴されたり，改ざんされる可能性がある．また第三者が成りすまして取引を行なう可能性もある．また取引に関与する当事者がデータを改ざんしたり，取引内容を否定したり，代金を持ち逃げしたりする可能性がある．既存のシステムでは，これらの問題に対応するために，データの暗号化，デジタル署名，認証局などを利用している．データの暗号化方式には，ＤＥＳ(DataEncryption Standard)やＲＳＡなどがある．これらの技術を利用した代表的なプロトコルとして，ＶＩＳＡ社とＭａｓｔｅｒｃａｒｄ社が開発したクレジットカード決済を対象としたセキュア電子取引プロトコル（ＳＥＴ）がある．暗号化方式，デジタル署名方式，認証局方式については，ＳＥＴの仕様書に記載されている．また電子マネーシステムとしては，Ｄｉｇｉｃａｓｈ社のｅｃａｓｈ，Ｍｏｎｄｅｘ社のＭｏｎｄｅｘマネーなどがある．Ｍｏｎｄｅｘ社の基本特許として特表平５－５０４６４３がある．

【０００３】

【発明が解決しようとする課題】既存のオープンネットワーク対応のショッピングシステムや，電子マネーシステムでは，通信中のデータの盗聴や改ざんを防止するために，暗号化やデジタル署名を利用している．ＳＥＴはクレジットカード決済を前提とした取引プロトコルであり，オープンネットワーク上では小売店に対する発注処理とカード会社に対する承認処理だけを行ない，決済処理は既存の金融ネットワークで行なっている．この場合，取引内容を証明する請求書はカード所有者に郵送され，決済が完了したことは，銀行口座からの引き落とし記録で立証できる．オープンネットワーク上で電子マネーを利用して取引する場合には，基本的に全ての処理は決済処理も含め，オープンネットワーク上で実行される．そこで取引内容や決済が完了したことを客観的に証明できる電子データをオープンネットワーク上で提供する必要がある．これらのデータは，通信途中で第三者によって書き換えられては困るし，またそれらのデータを受取った取引当事者によって自分の都合のよいように勝手に書き換えられても困る．また信用を有する第三者機関が決済の代行を行なう場合，注文を行う情報処理装置（発注クライアント）と，注文を受けつけたり注文を管理する情報処理装置（注文管理サーバ）と，代金を受領して管理する情報処理装置（決済サーバ）がそれぞれ独立にネットワークに接続される．この場合，注文情報や決済情報が改ざんされることなくこれらの情報処理装置間で転送され，かつ後日何か問題が発生した場合には，取引関与者がこれらの注文情報や決済情報を提示することで注文内容や決済完了を確認できたり，それらが改ざんされていないことを証明できる手段が必要である．さらに商品を購入する場合のみならず，商品を返品したり取引をキャンセルした場合に，オープンネットワーク上で電子マネーを使用して購入者に代金を払い戻せる必要がある．この場合，第三者が不正に払戻金を受け取ることがないようにする必要がある．本発明の目的は，オープンネットワーク上で電子マネーを使用してショッピングを行う場合に，ネットワーク上で取引内容や決済状態を証明するデータを取引関与者に提供する手段を提供することにある．本発明の別の目的は，注文する情報処理装置と，注文を受けつけ管理する情報処理装置と，代金を受領および管理する情報処理装置が独立にネットワークに接続されている場合に，取引上のトラブルを回避する手段を提供することにある．さらに本発明の別の目的は，オープンネットワーク上で電子マネーを使用して購入者に代金を払い戻す場合に，不正に第三者によって払戻金を横取りされずに，正規の購入者に払い戻す手段を提供することにある．

【０００４】

【課題を解決するための手段】上記目的を達成するために，複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて，発注を行う第１の情報処理装置に電子マネーを送受信する手段と，注文データを送信するための手段と，請求書データや領収書データを送受信する手段を設け，注文を受け付け，管理する第２の情報処理装置に注文データを受信するための手段と，注文データを記憶するための手段と，少なくとも支払金額と支払先と取引を特定するための識別子を含むデータに第２の情報処理装置が有する秘密鍵で暗号

化したデジタル署名を添付した請求書データを発行するための手段と，請求書データを送信するための手段と，支払先のデジタル署名が添付された領収書データを受信して領収書の有効性をチェックするための手段を設け，代金を受領・管理する第３の情報処理装置に電子マネーを送受信するための手段と，決済データを記憶するための手段と，少なくとも領収金額と取引を特定するための識別子を含むデータに第３の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した領収書データを発行する手段と，領収書データを送信するための手段を設ける．請求書データと領収書データには，発行者のみが有する秘密鍵で暗号化されたデジタル署名が添付されているので，発行者以外が改造することは困難であり，商品購入者がこれらのデータを提示すれば，取引内容やその取引の決済が完了したなどを証明できる．さらに第１の情報処理装置が第２の情報処理装置に注文データを送信するステップと，第２の情報処理装置が注文データを受信した場合に第１の情報処理装置に請求書データを送信するステップと，第１の情報処理装置が請求書データを受信すると第３の情報処理装置に請求書データを送信するステップと，第３の情報処理装置の応答に対して第１の情報処理装置から第３の情報処理装置に電子マネーを送金するステップと，第３の情報処理装置が電子マネーを受信したら第１の情報処理装置に領収書を送信するステップと，第１の情報処理装置が領収書を受信したら，領収書を第２の情報処理装置に送信するステップを設ける．このことにより，発注のための第１の情報処理装置と，受注のための第２の情報処理装置と，代金を受領する第３の情報処理装置がそれぞれオープンネットワークに接続されている場合であっても，問題が発生した場合にその問題の所在を明確にすることが可能になる．また代金の払戻を行なうために，第１の情報処理装置に払戻要求を送信するための手段と，電子マネーを送受信する手段と，少なくとも取引を特定するための識別子と受領した払戻金額に関するデータで構成されるデータに第１の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した払戻領収書を発行するための手段と，払戻領収書を送信するための手段と，払戻許可データを送受信するための手段を設け，第２の情報処理装置に，払戻要求を受信するための手段と，注文データを記憶するための手段と，少なくとも取引を特定するための識別子と払戻金の受取人を特定するための識別子と払戻金額に関係する情報を含むデータに第２の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した払戻許可書データを発行するための手段と，払戻許可書データを送信するための手段を設け，第３の情報処理装置に，払戻許可書データを受信するための手段と，前記払戻許可書データの有効性をチェックするための手段と，電子マネーを格納するための手段と，電子マネーを送受信するための手段と，決済データを記憶するための手段を設ける．さらにオンラインショッピングシステムにおいて，第１の情報処理装置が第２の情報処理装置に払戻要求を送信するステップと，第２の情報処理装置が前記払戻要求を受信した場合に払戻許可データを発行して第１の情報処理装置に送信するステップと，第１の情報処理装置が払戻許可データを受信すると第３の情報処理装置に払戻許可データを送信するステップと，払戻許可データが有効である場合に第３の情報処理装置から第１の情報処理装置に電子マネーを送金するステップと，第１の情報処理装置が電子マネーを受信したら第３の情報処理装置に払戻領収書データを送信するステップを設ける．以上により，払戻を要求する情報処理装置と，注文データを管理していて払戻を受け付ける情報処理装置と，払戻金を送金する電子マネー決済サーバがそれぞれネットワークに接続されている場合であっても，正当な払戻受領者に払戻金を送金することが可能になるとともに，払戻金の授受に関してトラブルが発生した場合には，払戻許可データや払戻領収書データを提示することにより問題を解決することが可能になる．払戻許可データと払戻領収書データには，発行者のみが有する秘密鍵で暗号化されたデジタル署名が添付されているので，発行者以外が改造することは困難である．また払戻許可データには払戻を受領する人もしくは情報処理装置を特定するためのデータが入っているとともに，第１の情報処理装置が第３の情報処理装置に払戻許可データを送信する前に第１の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付するので，商品購入者以外が払戻金を不正に受け取ることを防止できる．さらに払戻許可データに使用する払戻金を受領する人もしくは情報処理装置を特定するデータとして，デジタル署名の正当性を証明するために認証局に登録された証書に含まれる人もしくは情報処理装置を特定するためのデータを使用すれば，払戻要求者と払戻を受領する権利を有する人との一致性を容易に検証できる．

【０００５】

【発明の実施の形態】以下，本発明に係るオンラインショッピングシステムの実施例を図面を参照しながら説明する．図１は，本発明の全体構成を表わす構成図である．１は商品やサービスを注文する情報処理装置（消費者クライアントと呼ぶ）であり，２は注文を受けつけ管理する情報処理装置（受注管理サーバと呼ぶ）であり，３は代金を受けつけ管理する情報処理装置（電子マネー決済サーバと呼ぶ）である．４は，前記１から３の情報処理装置を相互に接続しているコンピュータネットワークであり，代表例としてインタネットがある．図２は，消費者クライアント１の構成図である．１１は電子マネーを格納する電子マネー格納装置であり，ＩＣカード（スマートカードとも呼ぶ）である場合と，その他の外部記憶装置である場合がある．１２はコンピュータネットワークを介して，他の情報処理装置との通信を行う通

信装置であり，電子マネー，注文データ，請求書データ，領収書データなどを送受信するために使用する．１３は，プログラムや各種データを記憶する記憶装置であり，デジタル署名を行うための秘密鍵も記憶される．１４は，注文データ，請求書データ，領収書データなどを表示するための表示装置である．１５は，注文データなどを入力するための入力装置である．１６はプログラムを制御するための装置で，デジタル署名を作成，検証したり，入出力を制御したり，通信を制御したり，実行順序を制御する．図３は，受注管理サーバ２の構成図である．２１はプログラムや注文データや顧客データなどを記憶する記憶装置であり，デジタル署名に使用する秘密鍵も記憶される．２２は他の情報処理装置と通信するための通信装置であり，注文データ，請求書データ，領収書データなどを送受信するために使用する．２３は各種データを入力するための入力装置であり，２４は各種データを表示するための表示装置である．入力装置２３および表示装置２４はなくてもよい．２５はプログラムを制御するための装置であり，デジタル署名を作成，検証したり，入出力を制御したり，通信を制御したり，実行順序を制御する．図４は，電子マネー決済サーバ３の構成図である．３１は電子マネーを格納するための装置であり，電子マネー格納装置１１と同様に，ＩＣカードである場合とそれ以外の外部記憶装置である場合がある．３２は他の情報処理装置と通信するための通信装置であり，電子マネー，請求書データ，領収書データなどを送受信するために使用する．３３はプログラムや各種データを記憶する記憶装置であり，デジタル署名を行うための秘密鍵も記憶される．３４は各種データを入力するための入力装置であり，３５は各種データを表示するための表示装置である．表示装置３４および入力装置３５はなくてもよい．以下，本発明のオンラインショッピングシステムで，商品もしくはサービスを購入する場合（購入プロセスとも呼ぶ）と，払戻の場合（払戻プロセスとも呼ぶ）の２つの実施例について説明する．

（１）商品もしくはサービスを購入する場合（購入プロセス）

図５は購入プロセスにおけるメッセージ，請求書データ５１，領収書データ５３の流れを示すフロー図である．１１０から２２０はそれぞれ情報処理装置間で送受信されるメッセージを表わす．請求書データ５１に記されている「M」は受注管理サーバ２によってデジタル署名されたことを示す．５２は代金受取要求メッセージ１５０に消費者クライアント１によって添付されたデジタル署名である．領収書データ５３に記されている「P」は電子マネー決済サーバ３によってデジタル署名されたことを示す．請求書データ５１に記されている「C」５２は消費者クライアント１によってデジタル署名されたことを表わす。

【０００６】図６は請求書データ５１のデータ構造図，

図７は領収書データ５３のデータ構造図である．これらのデータ項目は例であり，これ以外のデータ項目が使用されてもよい．デジタル署名は，署名の対象となるデータのハッシュ値を計算し，ハッシュ値に秘密鍵で暗号化したものである．ハッシュ値を算出するために使用されるハッシュ関数にはＳＨＡ－１やＭＤ５などのアルゴリズムがある．また秘密鍵で暗号化する方法にはＲＳＡなどの非対称暗号アルゴリズムを使用する．またデジタル署名を検証するためには，秘密鍵と対になっている公開鍵でデジタル署名を復号化したデータと署名の対象となっている平文データのハッシュ値を計算したデータが一致するかどうかをチェックする．５５はデータブロック５４のハッシュ値に受注管理サーバ２が有する秘密鍵で暗号化したデジタル署名である．５８はデータブロック５７のハッシュ値に電子マネー決済サーバ３が有する秘密鍵で暗号化したデジタル署名である．図８は消費者クライアント１の処理手順を表わすフロー図である．図９は受注管理サーバ２の処理手順を表わすフロー図である．図１０は電子マネー決済サーバ３の処理手順を表わすフロー図である．図１１と図１２は受注管理サーバ２の記憶装置２１に記憶されている注文データ６１，６２である．図１３は電子マネー決済サーバ３の記憶装置３３に記憶されている決済データ６３である．以下，図５、８、９、及び１０を用いて、購入プロセスの処理手順を説明する．　消費者クライアント１で注文データが入力されると（ステップ３１０），取引相手を認証するために注文準備要求メッセージ１１０を受注管理サーバ２に送信し，受注管理サーバ２はメッセージを受信すると（ステップ５１０），消費者クライアント１に認証用証書を含む注文準備応答メッセージ１２０を送信する（ステップ５２０）．消費者クライアント１は，証書を使用して相手認証を行なうと（ステップ３２０），受注管理サーバ２に注文データを含む注文要求メッセージ１３０を送信する（ステップ３３０）．図１４に消費者クライアント１の表示装置に表示される注文データ画面の例を示す．受注管理サーバ２がメッセージ１３０を受信すると（ステップ５３０），注文データを記憶装置２１に格納して（ステップ５４０），請求書データ５１を作成し（ステップ５５０），消費者クライアント１に支払要求メッセージ１４０を送信する（ステップ５６０）．図１５は消費者クライアント１の表示装置に表示される請求書データ画面７２である．支払要求メッセージ１４０を受信したときに，画面７２を表示してもよい．消費者クライアント１がメッセージ１４０を受信すると（ステップ３４０），電子マネー決済サーバ３に請求書データ５１を含む代金受取要求メッセージ１５０にデジタル署名５２を添付して送信する（ステップ３５０）．電子マネーサーバ３が前記メッセージ１５０を受信したら（ステップ７１０），請求書データ５１とデジタル署名５２の有効性をチェックして（ステップ７２０），有効

である場合には（ステップ７３０），消費者クライアント１に送金開始許可を含む代金受取応答メッセージ１６０を送信する（ステップ７４０）．また請求書データ５１およびデジタル署名５２が有効でない場合には処理を終了する．ステップ７３０で有効性をチェックする方法には，請求書データ５１に受注管理サーバ２のデジタル署名５５が添付されているかどうか，請求書データ５１に含まれる支払者を特定するためのデータ（支払者ＩＤなど）とデジタル署名５２を署名した者が同一であるかどうかをチェックする方法などがある．消費者クライアント１が代金受取応答メッセージ１６０を受信し（ステップ３６０），メッセージ１６０の中に送金許可を示すデータが含まれている場合（ステップ３７０），電子マネー決済サーバ３に電子マネー１７０を送信する（ステップ３８０）．電子マネー決済サーバ３が電子マネー１７０を受信したら（ステップ７５０），記憶装置３３の決済データ６３を更新し，電子マネーを受領したことを示すメッセージ１８０を消費者クライアント１に送信する（ステップ７６０）．消費者クライアント１がメッセージ１８０を受信したら（ステップ３９０），電子マネー決済サーバ３に領収書データを要求するメッセージ１９０を送信する（ステップ４００）．電子マネー決済サーバ３がメッセージ１９０を受信したら（ステップ７７０），領収書データ５３を作成し（ステップ７８０），消費者クライアント１に領収書データ５３を含む領収書応答メッセージ２００を送信する（ステップ７９０）．消費者クライアント１がメッセージ２００を受信したら（ステップ４１０），領収書データ５３を含む支払応答メッセージ２１０を受注管理サーバ２に送信する（ステップ４２０）．図１６は消費者クライアント１の表示装置に表示される領収書データ画面７３である．領収書応答メッセージ２００を受信したときに，画面７３を表示してもよい．受注管理サーバ２がメッセージ２１０を受信したら（ステップ５７０），領収書データ５３の有効性をチェックして（ステップ５８０），領収書データ５３が有効である場合には（ステップ５９０），記憶装置２１に格納されている注文データ６１を更新して（６００），消費者クライアント１に注文完了を示す注文応答メッセージ２２０を送信する（ステップ６１０）．領収書データ５３が有効でない場合には（ステップ５９０），消費者クライアント１に注文失敗を示す注文応答メッセージ２２０を送信する（ステップ６２０），ステップ５８０の有効性をチェックする方法には，領収書データ５３に請求書データ５１で指定した支払先のデジタル署名が添付されているかどうか，領収書データ５３に含まれる受賞金額に関するデータが代金の金額と一致するかどうかなどをチェックする方法がある．消費者クライアント１が受注管理サーバ２から注文応答メッセージ２２０を受信すると（ステップ４３０），購入プロセスが完了する．以上の処理により，消費者クライアント１，受注管理サーバ２，電子マネー決済サーバ３がそれぞれコンピュータネットワーク４に接続されている場合に安全に取引を行うことが可能になる．また請求書データ５１や領収書データ５３は，後日取引上の問題が起こった場合に取引内容や決済完了状態を示す証拠として使用することができる．さらに前記ステップ７２０により，電子マネー決済サーバ３への不正アクセスを防止することができる．

（２）払戻の場合（払戻プロセス）

図１７は払戻プロセスにおけるメッセージ，払戻許可書データ（払戻許可データとも呼ぶ）８１，払戻領収書８３の流れを示すフロー図である．１１１０から１２２０はそれぞれ情報処理装置間で送受信されるメッセージを表わす．払戻許可書データ８１に記されている「M」は受注管理サーバ２によってデジタル署名されたことを表わす．８２は払戻金送金要求メッセージ１１５０に消費者クライアント１によって添付されたデジタル署名である．払戻領収書８３に記されている「C」は消費者クライアント１によってデジタル署名されたことを表わす．図１８は払戻許可書データ８１のデータ構造図，図１９は払戻領収書８３のデータ構造図である．これらのデータ項目は例であり，他のデータ項目が使用されてもよい．８５はデータブロック８４のハッシュ値に受注管理サーバ２が有する秘密鍵で暗号化されたデジタル署名である．８８はデータブロック８７のハッシュ値に消費者クライアント１が有する秘密鍵で暗号化されたデジタル署名である．図２０は消費者クライアント１の処理手順を表わすフロー図である．図２１と図２２は受注管理サーバ２の処理手順を表わすフロー図である．図２３は電子マネー決済サーバ３の処理手順を表わすフロー図である．以下，図１７、２０、２１、２２、及び２３を用いて、払戻プロセスの処理手順を説明する．消費者クライアント１で払戻を行うために必要なデータを入力装置１５を用いて入力されると（ステップ１３１０），受注管理サーバ２に払戻要求メッセージ１１１０を送信する（ステップ１３２０）．図２４は前記消費者クライアント１の表示装置１４に表示される払戻要求するための画面９１である．受注管理サーバ２が前記メッセージ１１１０を受信したら（ステップ１５１０），メッセージで指定された取引ＩＤが払戻可能かどうかをチェックし（ステップ１５２０），可能であるならば電子マネー決済サーバ３に払戻準備要求メッセージ１１２０を送信する（ステップ１５３０）．電子マネー決済サーバ３がメッセージ１１２０を受信したら（ステップ１７１０），記憶装置３３に記憶されている決済データ６３を「払戻中」に更新して（ステップ１７２０）．受注管理サーバ２に準備完了を示す払戻準備応答メッセージ１１３０を送信する（ステップ１７３０）．受注管理サーバ２が応答メッセージ１１３０を受信したら（ステップ１５４０），記憶装置２１の注文データ６１を「払戻中」に更

新し（ステップ１５５０），払戻許可書データ８１を作成して（ステップ１５６０），消費者クライアント１に払戻許可書データ８１を含む払戻応答メッセージ１１４０を送信する（ステップ１５７０）．消費者クライアント１が応答メッセージ１１４０を受信したら（ステップ１３３０），応答メッセージ１１４０に含まれる払戻許可書データ８１を含む払戻金送金要求メッセージ１１５０に消費者クライアント１が有する秘密鍵で暗号化したデジタル署名８２を添付して電子マネー決済サーバ３に送信する（ステップ１３４０）．図２５は消費者クライアント１の表示装置１４に表示される払戻許可書データの画面９２である．払戻応答メッセージ１１４０を受信したときに画面９２を表示してもよい．電子マネー決済サーバ３が要求メッセージ１１５０を受信したら（ステップ１７４０），払戻許可書データ８１とデジタル署名８２を用いて払戻が可能かどうかチェックする（ステップ１７５０）．この場合のチェック方法として，払戻許可書データ８１に受注管理サーバ２のデジタル署名が添付されているか，払戻許可書データ８１で指定される払戻受領者がデジタル署名８２を署名した者と一致するかなどをチェックする方法がある．ステップ１７５０の結果が有効である場合には（ステップ１７６０），消費者クライアント１に払戻許可を示すデータを含む払戻金送金応答メッセージ１１６０を送信する（ステップ１７７０）．ステップ１７５０の結果が無効である場合には（ステップ１７６０），払戻不可を示すデータを含む払戻金送金応答メッセージ１１６０を消費者クライアント１に送信する（ステップ１８５０）．消費者クライアント１が応答メッセージ１１６０を受信し（ステップ１３５０），メッセージ１１６０に払戻許可を示すデータが含まれている場合には（ステップ１３６０），電子マネー決済サーバ３に電子マネー送金要求を示すメッセージ１１７０を送信する（ステップ１３７０）．ステップ１３６０でメッセージ１１６０に払戻不可を示すデータが含まれている場合には処理を終了する．電子マネー決済サーバ３がメッセージ１１７０を受信したら（ステップ１７８０），消費者クライアント１に電子マネー１１８０を送金する（ステップ１７９０）．消費者クライアント１が電子マネー１１８０を受信したら（ステップ１３８０），払戻領収書データ８３を作成して（ステップ１３９０），領収書データ８３を含む払戻領収書送信メッセージ１１９０を電子マネー決済サーバ３に送信する（ステップ１４００）．電子マネー決済サーバ３がメッセージ１１９０を受信したら（ステップ１８００），記憶装置３３に記憶されている決済データ６３を「払戻完了」に更新して（ステップ１８１０），払戻領収書応答メッセージ１２００を消費者クライアント１に送信する（ステップ１８２０）．消費者クライアント１が応答メッセージ１２００を受信したら（ステップ１４１０），処理を終了する．受注管理サーバ２は所定の時間が経過

したら電子マネー決済サーバ３に払戻状態要求メッセージ１２１０を送信する（ステップ１６１０）．電子マネー決済サーバ３が要求メッセージ１２１０を受信したら（ステップ１８３０），受注管理サーバ２に払戻完了状態を含む払戻状態応答メッセージ１２２０を送信する（ステップ１８４０）．このとき既に払戻が完了している場合には，応答メッセージ１２２０で消費者クライアント１から受け取った払戻領収書８３を送信してもよい．受注管理サーバ２は，応答メッセージ１２２０を受信したら（ステップ１６２０），記憶装置２１に記憶されている注文データ６１を「払戻完了」に更新して（ステップ１６３０），処理を終了する．以上の処理により，消費者クライアント１，受注管理サーバ２，電子マネー決済サーバ３がそれぞれコンピュータネットワーク４に接続されている場合に安全に電子マネーを用いて払い戻しすることが可能になる．また払戻許可書データ８１や払戻領収書データ８３は，後日払戻に関する問題が起こった場合に払戻内容や払戻完了状態を示す証拠として使用することができる．さらにステップ１７５０により，電子マネー決済サーバ３への不正アクセスを防止することができるとともに，他人が不正に払戻金を受け取ることを防止できる．図８又は２０に示した処理を実行するプログラムをフロッピィディスクなどの可搬記憶媒体に格納し、これを消費者クライアント１の記憶部１３に読み込んで実行することも可能である。受注管理サーバ２、及び電子マネー決済サーバ３についても同様である。

【０００７】

【発明の効果】オープンネットワーク上で電子マネーを使用してショッピングを行ない，後日問題が発生した場合に取引関与者が取引内容や決済状態を証明することが可能になる．また第三者が不正に取引に介入することを防止できる．さらにオープンネットワーク上で電子マネーを使用して代金の払戻を安全に行うことができる．

【図面の簡単な説明】

【図１】本発明の全体構成を表わす構成図である。

【図２】消費者クライアント１の構成図である。

【図３】受注管理サーバ２の構成図である。

【図４】電子マネー決済サーバ３の構成図である。

【図５】購入プロセスのメッセージ，請求書データ５１，領収書データ５３のフロー図である。

【図６】請求書データ５１のデータ構造図である。

【図７】領収書データ５３のデータ構造図である。

【図８】購入プロセスにおける消費者クライアント１の処理フロー図である。

【図９】購入プロセスにおける受注管理サーバ２の処理フロー図である。

【図１０】購入プロセスにおける電子マネー決済サーバ３の処理フロー図である。

【図１１】受注管理サーバ２の記憶装置２１に記憶され

15

ている注文データ構造６１である。

【図１２】受注管理サーバ２の記憶装置２１に記憶されている注文データ構造６２である。

【図１３】電子マネー決済サーバ３の記憶装置３３に記憶されている決済データ構造６３である。

【図１４】注文データが表示されている消費者クライアント画面７１である。

【図１５】請求書データ５１が表示されている消費者クライアント画面７２である。

【図１６】領収書データ５３が表示されている消費者クライアント画面７３である。

【図１７】払戻プロセスのメッセージ，払戻許可データ８１，払戻領収書データ８３のフロー図である。

【図１８】払戻許可書データ８１のデータ構造図である。

【図１９】払戻領収書データ８３のデータ構造図である。

【図２０】払戻プロセスにおける消費者クライアント１の処理フロー図である。

【図２１】払戻プロセスにおける受注管理サーバ２の処理フロー図である。

【図２２】払戻プロセスにおける受注管理サーバ２の処理フロー図である。

【図２３】払戻プロセスにおける電子マネー決済サーバ３の処理フロー図である。

【図２４】払戻要求書データが表示されている消費者クライアント画面９１である。

【図２５】払戻許可書データ８１が表示されている消費者クライアント画面９２である。

【符号の説明】

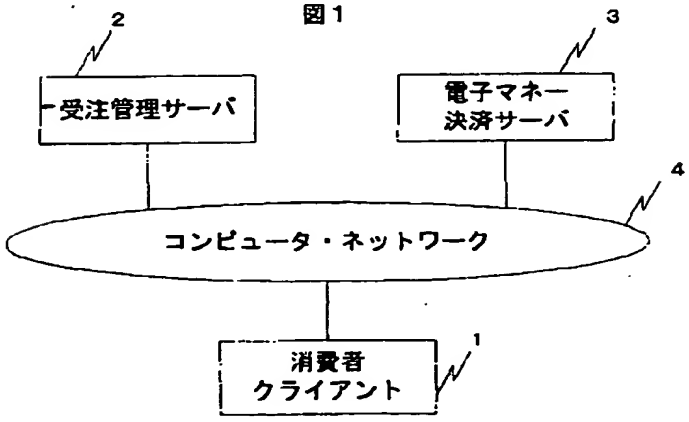
１…消費者クライアント，２…受注管理サーバ，３…電

16

子マネー決済サーバ，４…コンピュータネットワーク，１１から１６…消費者クライアントの構成要素，２１から２５…受注管理サーバの構成要素，３１から３６…電子マネー決済サーバの構成要素，５１…請求書データ，５２…消費者クライアント１のデジタル署名，５３…領収書データ，５４…請求書データの平文データブロック，５５…データブロック５４に対するデジタル署名，５７…領収書データの平文データブロック，５８…データブロック５７に対するデジタル署名，６１，６２…受注管理サーバに記憶されている注文データ，６３…電子マネー決済サーバに記憶されている決済データ，７１…注文データ画面，７２…請求書画面，７３…領収書画面，８１…払戻許可書データ，８２…消費者クライアント１のデジタル署名，８３…払戻領収書データ，８４…払戻許可書データの平文データブロック，８５…データブロック８４に対するデジタル署名，８７…払戻領収書データの平文データブロック，８８…データブロック８７に対するデジタル署名，９１…払戻要求書画面，９２…払戻許可書画面，１１０から２２０…購入プロセスで使用される通信メッセージ，３１０から４３０…購入プロセスにおける消費者クライアント１の処理ステップ，５１０から６１０…購入プロセスにおける受注管理サーバ２の処理ステップ，７１０から７９０…購入プロセスにおける電子マネー決済サーバ３の処理ステップ，１１１０から１２２０…払戻プロセスで使用される通信メッセージ，１３１０から１４１０…払戻プロセスにおける消費者クライアント１の処理ステップ，１５１０から１６３０…払戻プロセスにおける受注管理サーバ２の処理ステップ，１７１０から１８５０…払戻プロセスにおける電子マネー決済サーバ３の処理ステップ

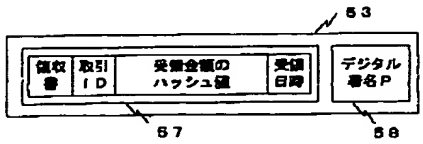
【図１】

図１



【図７】

図7



【図１１】

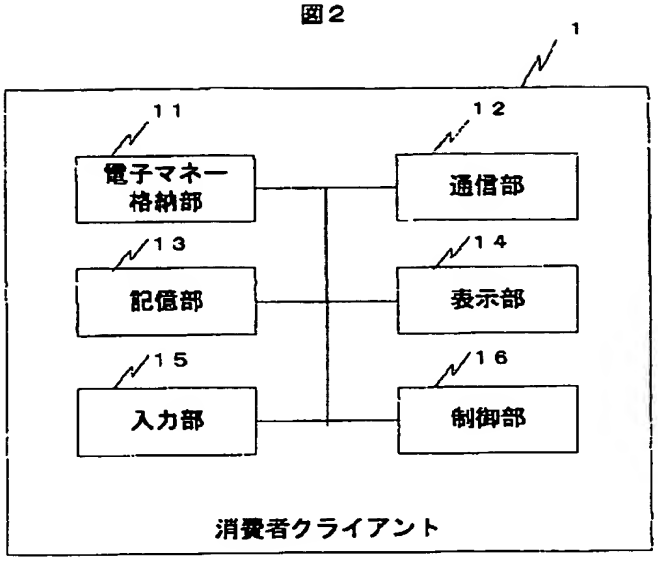
図11

61

取引ID	購入者ID	代金合計	決済方法	決済状態
210191	9821358	5，000	クレジットA	決済完了
210192	8790392	2，500	電子マネー	決済完了
210193	3789617	4，000	電子マネー	承認完了
210194	4789711	1，000	電子マネー	決済未完
210195	1789090	4，000	クレジットB	承認完了
⋮	⋮	⋮	⋮	⋮

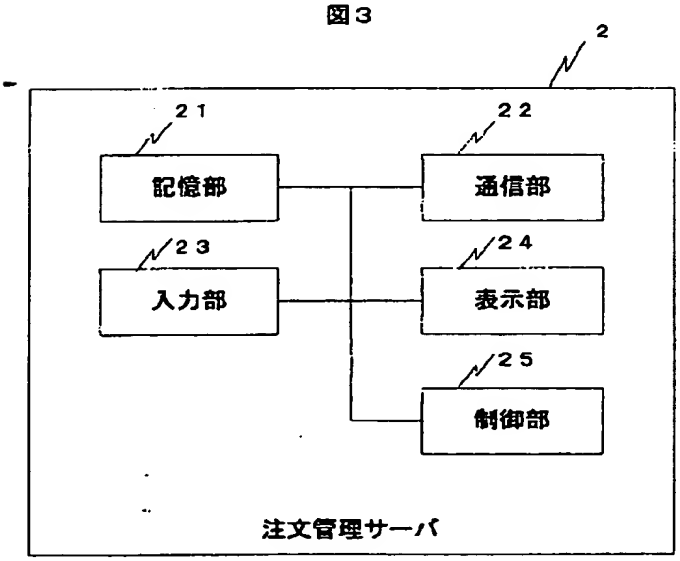
【図２】

図２



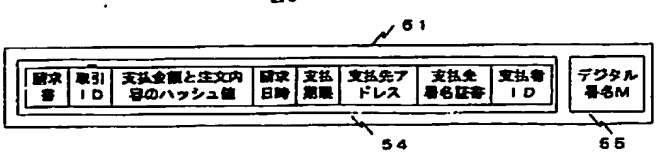
【図３】

図３



【図６】

図６



【図１２】

図１２

62

取引ＩＤ	商品名	個数	単価	金額
210191	商品A	1	1,000	1,000
	商品B	2	2,000	4,000
210192	商品C	1	2,500	2,500
210193	商品A	1	1,000	1,000
	商品C	1	1,500	3,000
210194	商品A	1	1,000	1,000
210196	商品B	2	2,000	4,000
:	:	:	:	:

【図１３】

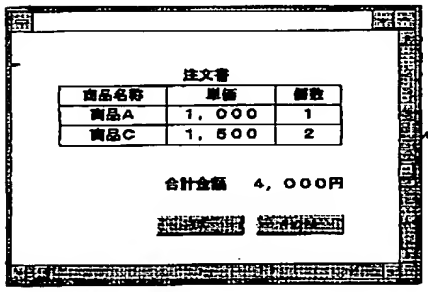
図１３

63

取引ＩＤ	購入者ＩＤ	小売店ＩＤ	代金合計	決済状態
210192	8790392	1230001	2,500	決済完了
210193	3090890	1230001	4,000	決済完了
210194	4789711	1230001	1,000	決済未完
120930	4343290	0090800	2,300	決済未完
230090	1343222	0900202	3,200	決済未完
:	:	:	:	:

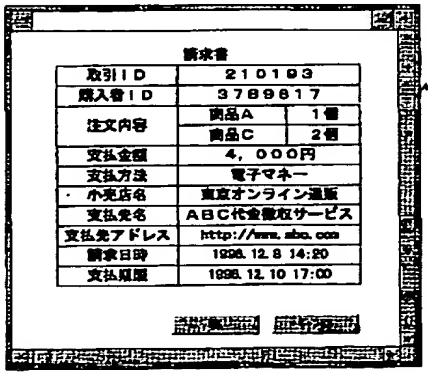
【図１４】

図１４



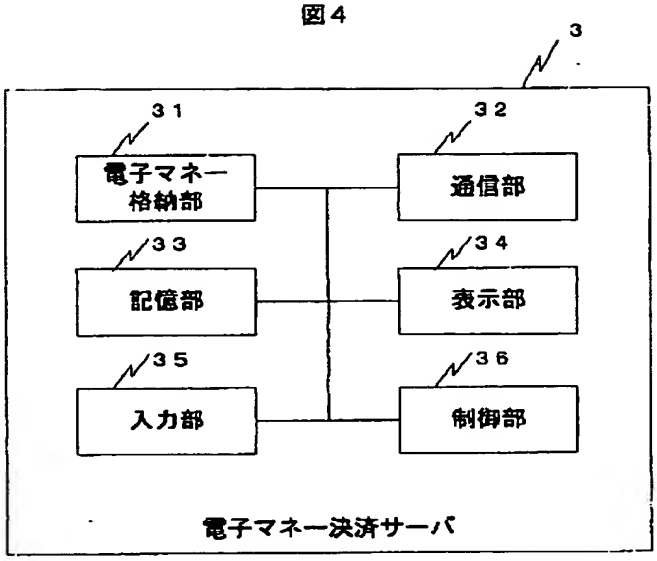
【図１５】

図１５



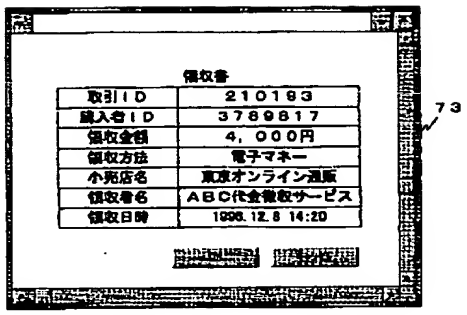
【図４】

図４



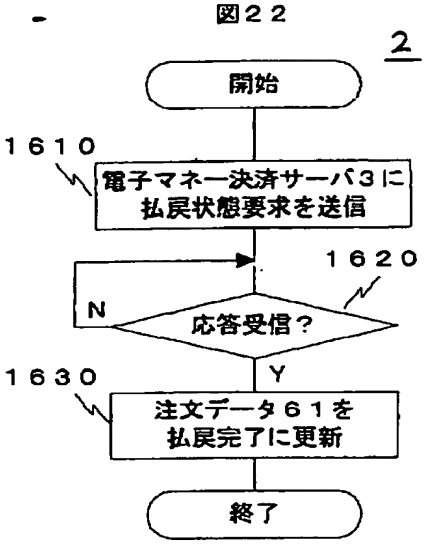
【図１６】

図16



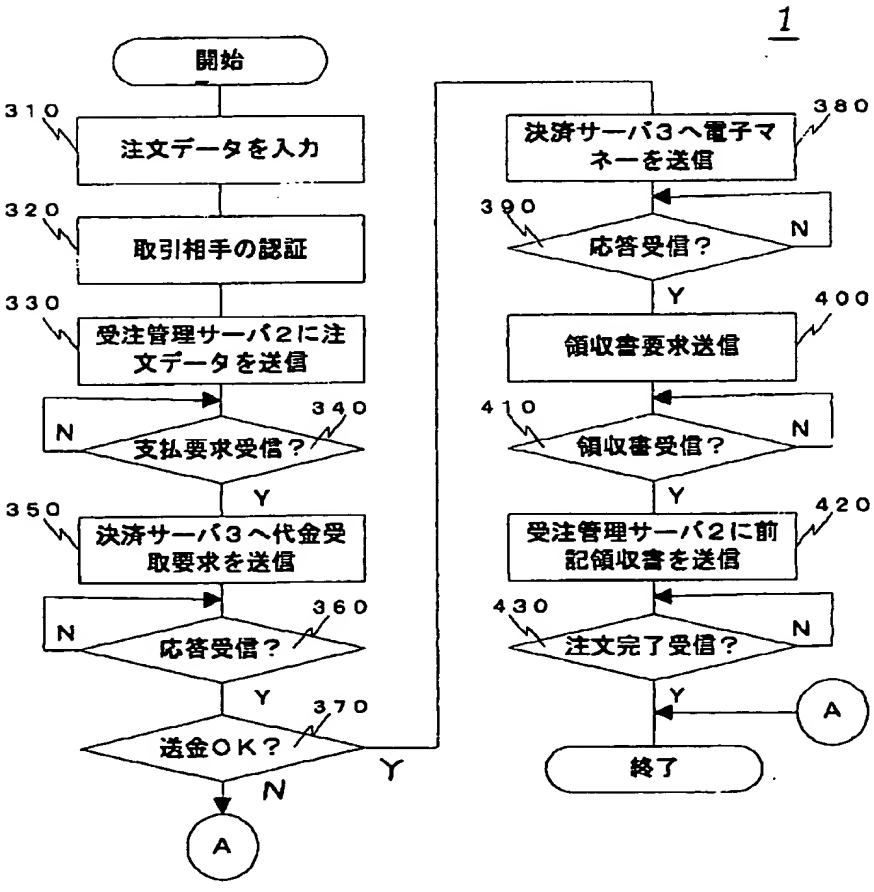
【図２２】

図２２



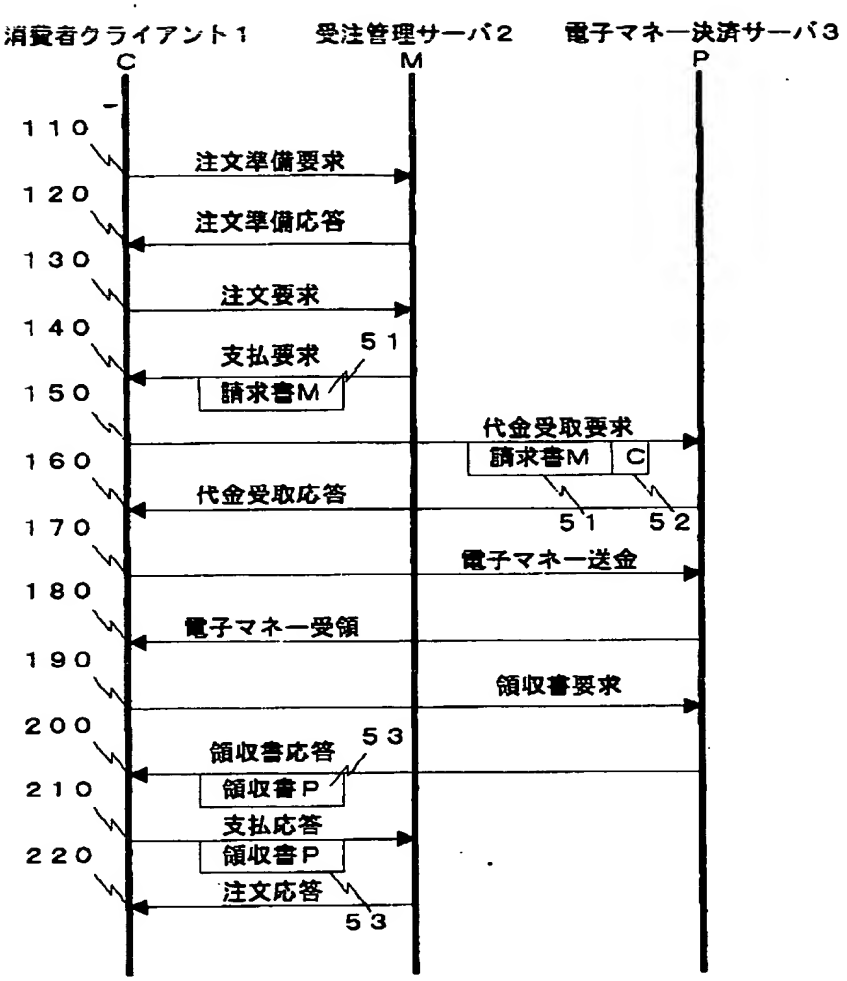
【図８】

図８



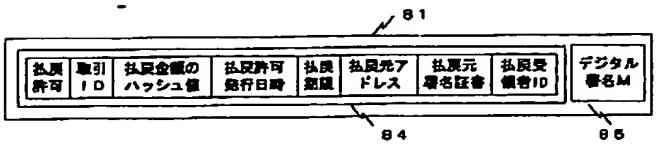
【図５】

図５



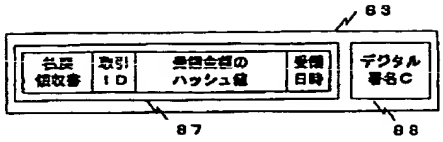
【図１８】

図18



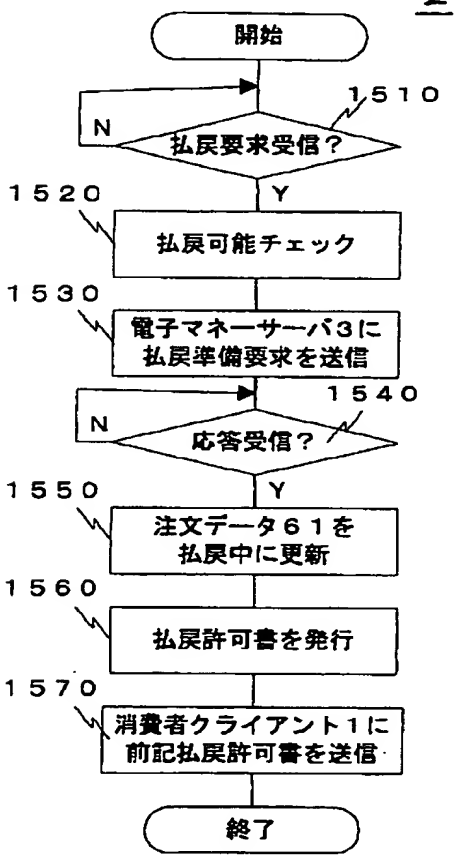
【図１９】

図19



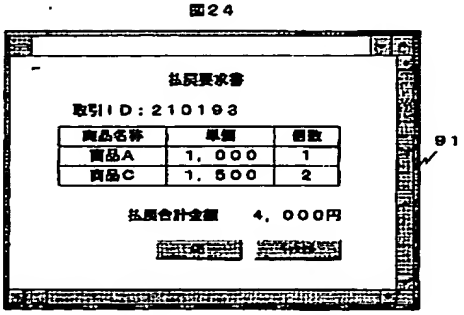
【図２１】

図２１



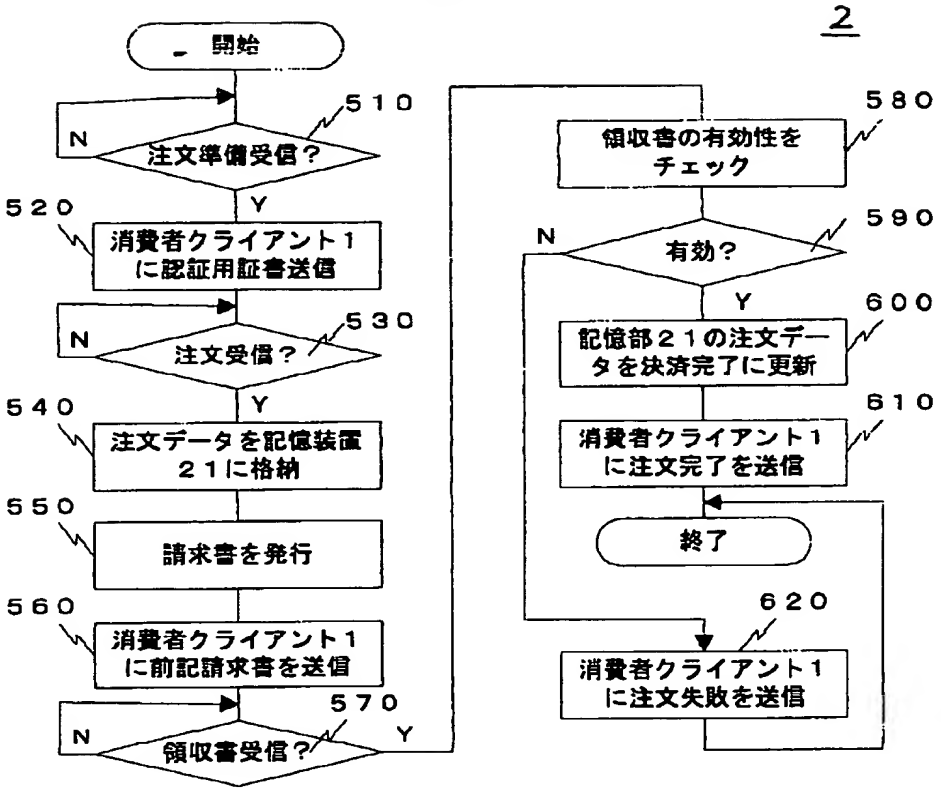
【図２４】

図24



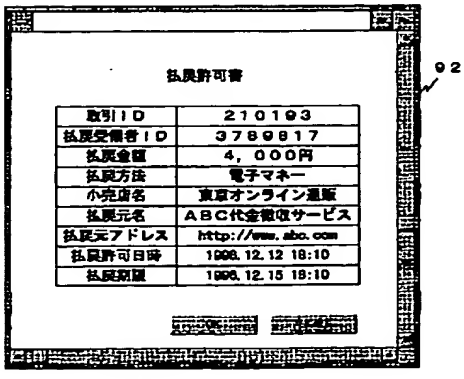
【図９】

図９


2
開始
510
N
注文準備受信？
Y
520
消費者クライアント１に認証用証書送信
530
N
注文受信？
Y
540
注文データを記憶装置２１に格納
550
請求書を発行
560
消費者クライアント１に前記請求書を送信
570
N
領収書受信？
Y
580
領収書の有効性をチェック
590
N
有効？
Y
600
記憶部２１の注文データを決済完了に更新
610
消費者クライアント１に注文完了を送信
終了
620
消費者クライアント１に注文失敗を送信

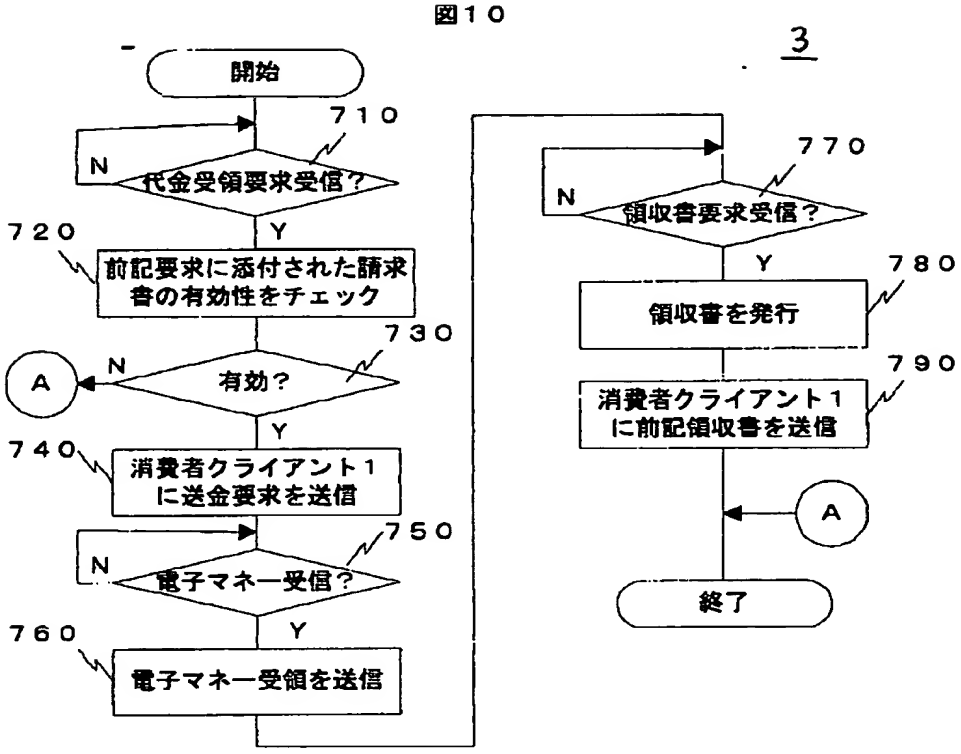
【図２５】

図２５


払戻許可書
92
取引ＩＤ　210193
払戻受信者ＩＤ　3789817
払戻金額　4，000円
払戻方法　電子マネー
小売店名　東京オンライン直販
払戻元名　ＡＢＣ代金徴収サービス
払戻元アドレス　http://www.abc.com
払戻許可日時　1998.12.12 18:10
払戻期限　1998.12.15 18:10

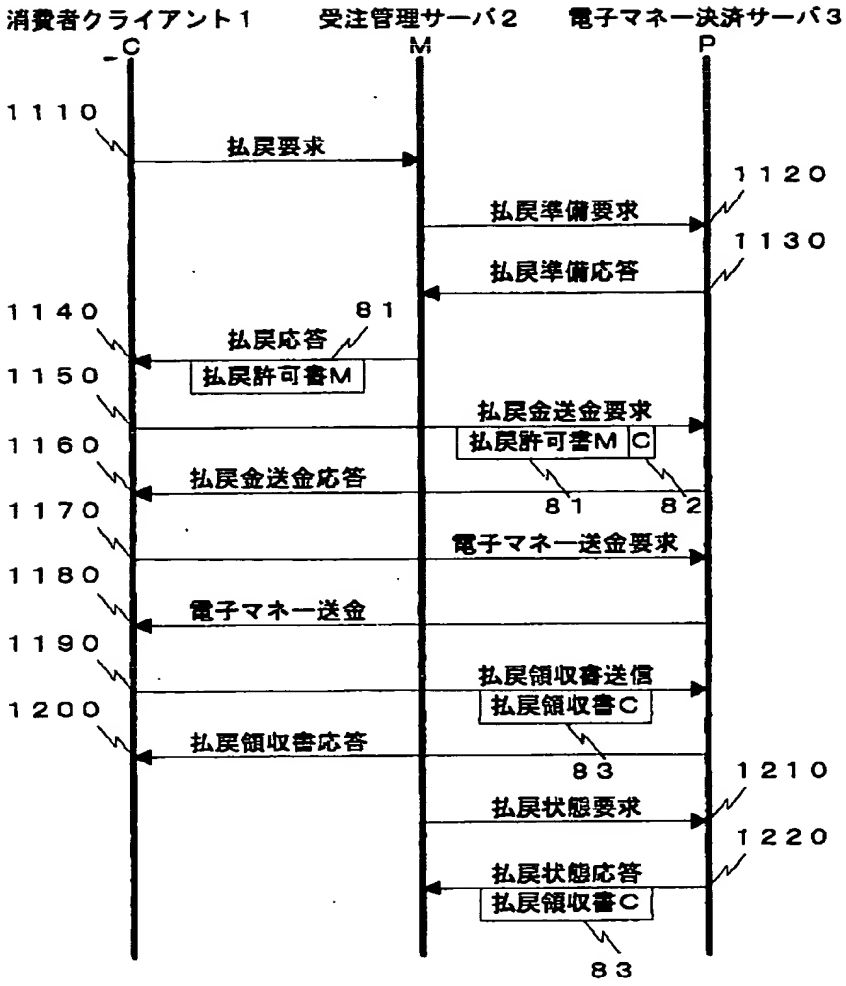
【図１０】

図１０


3
開始
710
N
代金受領要求受信？
Y
720
前記要求に添付された請求書の有効性をチェック
730
A
N
有効？
Y
740
消費者クライアント１に送金要求を送信
750
N
電子マネー受信？
Y
760
電子マネー受領を送信
770
N
領収書要求受信？
Y
780
領収書を発行
790
消費者クライアント１に前記領収書を送信
A
終了

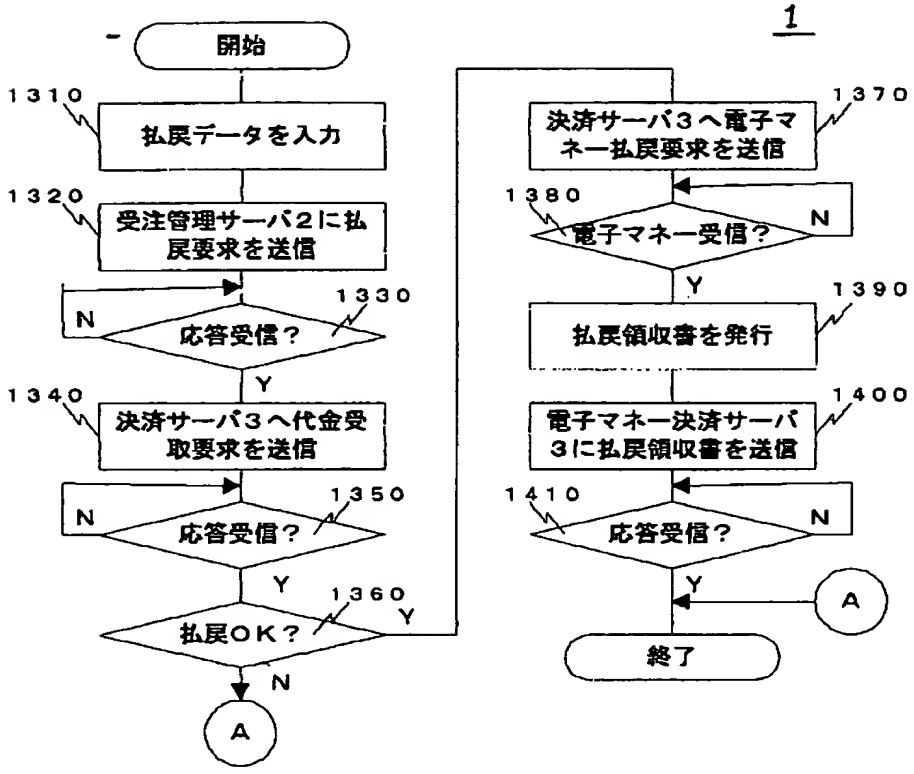
【図１７】

図１７


消費者クライアント１
受注管理サーバ２
電子マネー決済サーバ３
C
M
P
１１１０
払戻要求
１１２０
払戻準備要求
１１３０
払戻準備応答
１１４０
８１
払戻応答
払戻許可書Ｍ
１１５０
払戻金送金要求
払戻許可書Ｍ
C
１１６０
払戻金送金応答
８１
８２
１１７０
電子マネー送金要求
１１８０
電子マネー送金
１１９０
払戻領収書送信
払戻領収書Ｃ
１２００
払戻領収書応答
８３
１２１０
払戻状態要求
１２２０
払戻状態応答
払戻領収書Ｃ
８３

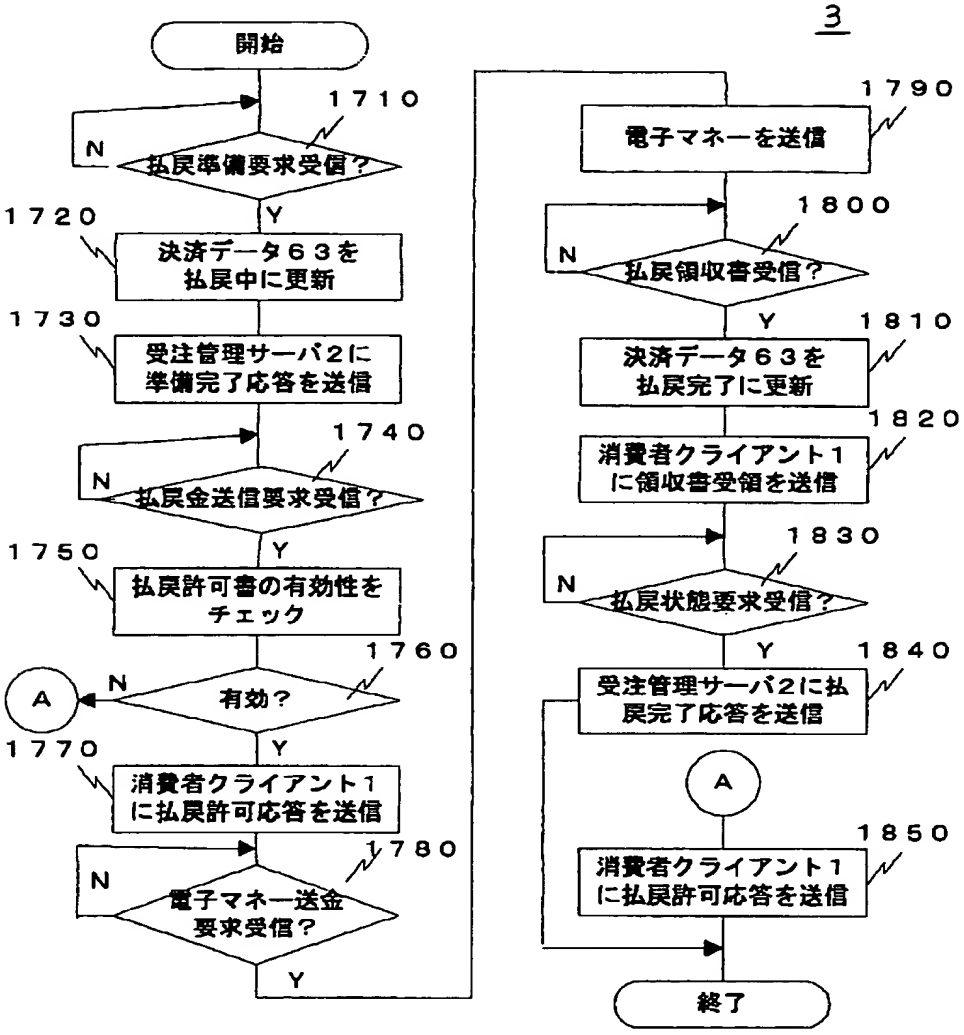
【図２０】

図２０


1
開始
1310
払戻データを入力
1320
受注管理サーバ２に払戻要求を送信
1330
応答受信？
N
Y
1340
決済サーバ３へ代金受取要求を送信
1350
応答受信？
N
Y
1360
払戻ＯＫ？
Y
N
A
1370
決済サーバ３へ電子マネー払戻要求を送信
1380
電子マネー受信？
N
Y
1390
払戻領収書を発行
1400
電子マネー決済サーバ３に払戻領収書を送信
1410
応答受信？
N
Y
A
終了

【図２３】

図２３



フロントページの続き

(72)発明者　伊藤　淳史
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　川連　嘉晃
神奈川県横浜市都筑区加賀原二丁目２番株式会社日立製作所ビジネスシステム開発センタ内
(72)発明者　寺村　健
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　富山　朋哉
神奈川県横浜市都筑区加賀原二丁目２番株式会社日立製作所ビジネスシステム開発センタ内